National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

SonicWall SMA v12.4

Report Number: CCEVS-VR-VID11527-2024

Version: 1.0

Date: August 14, 2024

National Institute of Standards and Technology

Information Technology Laboratory

100 Bureau Drive

Gaithersburg, MD 20899

Department of Defense

Attn: NIAP, Suite 6982

9800 Savage Road

Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Russell Fink

Daniel Faigin

Patrick Mallett, PhD

Common Criteria Testing Laboratory

Nithya Rachamadugu

Diego Sierra Liras

DEKRA Cybersecurity Certification Laboratory,

Sterling, Virginia, USA

Table of Contents

Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of SonicWall SMA v12.4, provided by SonicWall. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the DEKRA Cybersecurity Certification Common Criteria Testing Laboratory (CCTL) in Sterling, Virginia, United States of America, and was completed in August 2024. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by DEKRA. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements set forth in the *collaborative Protection Profile for Network Devices v2.2e [NDcPP]*.

The TOE, SonicWall v12.4.3, is a network device product. The TOE's primary purpose provides a minimal set of security requirements expected by all Network Devices that target the mitigation of a set of defined threats.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5), as interpreted by the Assurance Activities contained in the [NDcPP].

This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units of the ETR for the [NDcPP] Assurance Activities. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the SonicWall SMA v12.4 Security Target version 1.2, August 14, 2024, and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities that are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance results of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1 – Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	SonicWall Secure Mobile Access (SMA) v12.4
Protection Profile	collaborative Protection Profile for Network Devices v2.2e [NDcPP]
Security Target	SonicWall SMA v12.4 Security Target version 1.2, August 14, 2024
Evaluation Technical Report	Part-1 SonicWall SMA 12.4.3 - ND cPP ETR v0.8, August 14, 2024 Part-2 SonicWall SMA 12.4.3 - ND cPP ETR v0.5, August 14, 2024
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5
Conformance Result	CC Part 2 extended; CC Part 3 conformant

Sponsor	SonicWall, Inc.
Developer	SonicWall, Inc.
Common Criteria Testing Lab (CCTL)	DEKRA Cybersecurity Certification, Sterling, Virginia, USA
CCEVS Validators	Russell Fink Daniel Faigin Patrick Mallett

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

3.1 TOE Product Type

The Target of Evaluation [TOE] is a Network Device as defined by the collaborative Protection Profile for Network Devices v2.2e [NDcPP]: "A network device in the context of this cPP is a device composed of both hardware and software that is connected to the network and has an infrastructure role within the network".

3.2 TOE Evaluated Configuration

The evaluated configuration consists of the hardware and software listed below when configured in accordance with the documentation specified in section 6.

3.2.1 Hardware

Platform	Model	OS	CPU	RAM	Form	Specs
SMA v12.4.3	SMA 6210	SMA1000	Intel Core i5-7500 (Kaby Lake)	8GB (DDR4)	1U	6 1GB Ports
	SMA 7210	SMA1000	Intel Xeon E3-1275 v6 (Kaby Lake)	16GB (DDR4)	1U	6 1GB, 2 10GB SFP+ Ports

3.2.2 Software

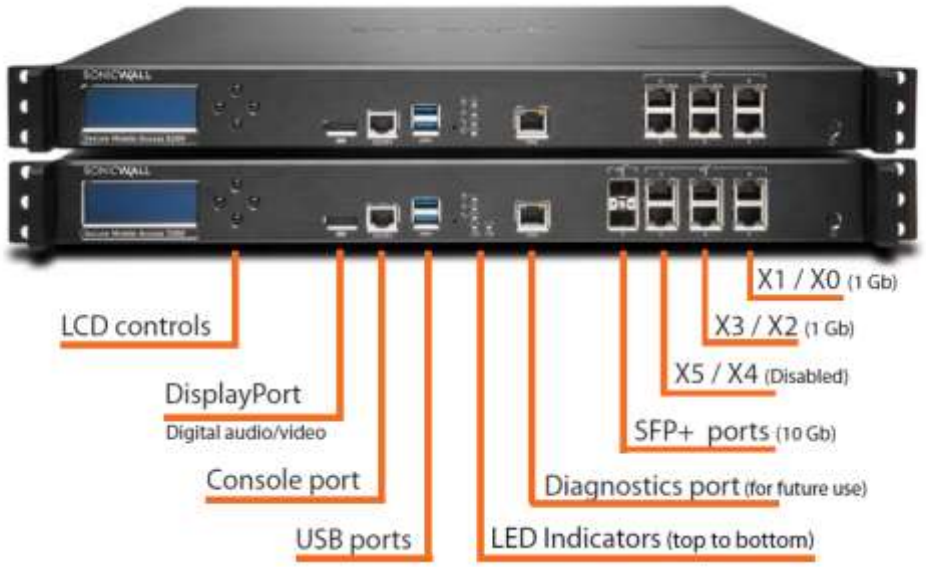
The TOE, SonicWall SMA v12.4, is offered as SMA 6210 and SMA 7210 hardware appliances and SMA 8200v virtual appliance. The TOE's firmware is consistent across all appliances and consists of multiple components, including SonicWall Operating System (SMA1000). SonicWall Operating System, SMA1000, is based on Linux 5.10 kernel. The firmware assigned a uniquely identifiable build number and is the same for each appliance.

3.2.3 Virtualization

The TOE, SonicWall SMA v12.4, includes SMA 8200v virtual appliance. While SMA 8200v can be installed on a variety of hypervisors, it was only evaluated using the VMware ESXi 7.0.3u hypervisor running on a general-purpose PC, with the following virtual system specification:

Platform	Model	Hypervisor	OS	CPU	RAM	Hard disk space	Virtual NIC
SMA v12.4.3	SMA 8200v	ESXi 7.0.3u	SMA1000	4 vCPUs (Intel Xeon Gold 5315Y 3.20GHz)	8GB ECC DDR-4 2400	160 GB, thick provisioned	2 vNIC of 1000BaseT

3.2.4 Physical Interfaces



4 Assumptions and Clarification of Scope

4.1 Assumptions

This section identifies assumptions applicable to the NDcPP, as specified in the Protection Profile, verbatim.

- A.PHYSICAL_PROTECTION: The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
- A.LIMITED_FUNCTIONALITY: The device is assumed to provide networking functionality as its core function and not provide functionality/ services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality).
- If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.
- A.NO_THRU_TRAFFIC_PROTECTION: A standard/generic network device does not

provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs for particular types of Network Devices (e.g., firewall).

- A.TRUSTED_ADMINISTRATOR: The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.
- For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
- A.REGULAR_UPDATES: The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
- A.ADMIN_CREDENTIALS_SECURE: The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
- A.RESIDUAL_INFORMATION: The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
- A.VS_TRUSTED_ADMINISTRATOR: The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.
- A.VS_REGULAR_UPDATES: The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
- A.VS_ISOLATION: For vNDs, it is assumed that VS provides, and is configured to provide sufficient isolation between software running in VMs one the same physical platform. Furthermore, it is assumed that the VS adequately protects itself form software running inside VMs on the same physical platform.
- A.VS_CORRECT_CONFIGURATION: For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.**Threats**

The following lists the threats addressed by the TOE. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

- T.UNAUTHORIZED_ADMINISTRATOR_ACCESS: Threat agents may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.

- T.WEAK_CRYPTOGRAPHY: Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.

- T.UNTRUSTED_COMMUNICATION_CHANNELS: Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.

- T.WEAK_AUTHENTICATION_ENDPOINTS: Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.

- T.UPDATE_COMPROMISE: Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

- T.UNDETECTED_ACTIVITY: Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.

- T.SECURITY_FUNCTIONALITY_COMPROMISE: Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.

- T.PASSWORD_CRACKING: Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow

them to take advantage of any trust relationships with other Network Devices.

- T.SECURITY_FUNCTIONALITY_FAILURE: An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

4.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Protection Profile for Network Devices, Version 2.2e [NDcPP]
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor serious attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication, and resources.

The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security-related functional capabilities included in the product were not covered by this evaluation.

The TOE supports several features that are not part of the evaluated functionality. These features are not tested and excluded from the scope of the evaluation:

- The integration with a domain controller was not evaluated
- Any integration and/or communication with a single sign-on (SSO) provider was excluded from the evaluated configuration, including dynamic SSO profile.
- The use of the SNMP management functionality is excluded, and it is disabled by default. The use of SNMPv3 for monitoring is not restricted; however, it is not evaluated.
- The use of SMTP is not evaluated and should not be configured in the evaluated configuration.
- The TOE supports IPv6 functionality; however, it is not evaluated.
- The remote access to CLI over SSH is not evaluated and not enabled in the evaluated configuration.
- The remote access to CLI via hypervisor console emulation is not evaluated, this configuration and mode of access is controlled by hypervisor software.
- The synchronization with an NTP server is not evaluated.
- The extraWeb and the WorkPlace interfaces and all relevant end-user functionality is not evaluated.

- The interoperability with additional VPN clients, other than Connect Tunnel on Windows, is not evaluated
    - The access Policy setting, and enforcement is not evaluated
    - The File Share functionality is not evaluated
    - The OnDemand Tunnel Agent is not evaluated
    - The Mobile Connect App integration is not evaluated
    - The Web Proxy Agent is not evaluated
- Limited controls via physical buttons on hardware appliance were not evaluated.
- The separation of security domains within SMA appliance was not evaluated, single-domain mode was configured and utilized throughout testing.
- The TOE was tested using the internal interface that corresponds with a single-homed configuration, the external interface of a dual-homed configuration was not evaluated.
- The support for TLS 1.3 was not evaluated as corresponding SF and AAs are still being developed by NDcPP iTC and are not available in the current version of the cPP.
- The support for hypervisors other than ESXi was not evaluated.
- Splunk Add-on integrated in the Splunk Server is not evaluated.
- Integration of SMA with Cisco Duo Security MFA Server is not evaluated.
- Integration of SMA with RSA SecurID Authentication Manager is not evaluated.
- Microsoft Intune integration is not evaluated.
- Client application Secure Endpoint Manager (SEM) is not evaluated.

5 Security Policy

5.1 Security Audit

The TOE generates audit records for all security-relevant events. For each event, the TOE records the date and time, the type of event, the subject identity, and the outcome of the recoded event. The resulting records can be stored locally or securely sent to a designated audit server for archiving. Security Administrators using the appropriate AMC menu can also view audit records locally. The TOE also implements timestamps based on a local system clock to ensure reliable audit information produced.

5.2 Cryptographic Support

The TOE performs the following cryptographic functionality:

- Encryption, decryption, hashing, keyed-hash message authentication, random number generation, signature generation and verification utilizing dedicated cryptographic library.
- Cryptographic functionality is utilized to implement secure channels.
    - TLSv1.2
- Entropy is collected from multiple entropy sources and used to support PRNG seeding with full entropy.
- Critical Security Parameters (CSPs) internally stored and cleared when no longer in use.
- X.509v3 certificate-based authentication integrated with TLS protocol.

The TOE is certified as a FIPS 140-2 level 2 cryptographic module, it internally manages CSPs and implements deletion procedures to mitigate the possibility of disclosure or modification of CSPs. Additionally, the TOE provides functionality to manually clear CSPs (e.g. host RSA keys), that can be invoked by a Security Administrator with appropriate permissions.

5.3 Identification and Authentication

The TOE supports Role-Based Access Control (RBAC) managed by an AAA module that stores and manages permissions of all users and their roles. Before any other action, each user is identified with a login name and authenticated with a password. Each authorized user is associated with assigned role and specific permissions that determine access to TOE features.

5.4 Security Management

The TOE allows remote administration using a TLS session over an internal management Ethernet port and local administration using a console adapter via a separate RJ-45 running RS-232 signaling. Remote administration is conducted over web-based interface (AMC) and local administration conducted over CLI.

All of the management functionality is restricted to the Security Administrators of the TOE. The Security Administrators are authorized to perform configuration and management of the TOE. The term “Security Administrator” is used to refer to any user with an administrative role and sufficient permissions.

5.5 Protection of the TSF

The TOE implements a number of measures to protect the integrity of its security features. The TOE protects CSPs, including stored passwords and cryptographic keys, so they are not directly viewable in plaintext. The

TOE also ensures that reliable time information is available for both log accountability and synchronization with the operating environment.

The TOE employs both dedicated communication channels as well as cryptographic means to protect the communication between itself and the other components in the operational environment.

The TOE performs self-tests to detect internal failures and to protect itself from malicious updates.

5.6 TOE Access

The TOE will display a customizable banner when an administrator initiates an interactive local or remote session. The TOE also enforces an administrator-defined inactivity timeout after which the inactive session is automatically terminated. Once a session (local or remote) has been terminated, the TOE requires the user to re-authenticate.

5.7 Trusted Path/Channels

The TOE protects remote sessions by establishing a trusted path secured with TLS between itself and the administrator. The TOE prevents disclosure or modification of audit records by establishing a trusted channel secured with TLS between itself and the audit server.

6 Documentation

The vendor provides a standard set of guidance documents that covers the core functionality of the product. These documents were used during the evaluation of the TOE:

- SonicWall Secure Mobile Access 12.4.3 Administration Guide
- SonicWall SMA v12.4, Common Criteria Configuration Guide, Version 6.0

These guidance documents contain the security-related guidance material for this evaluation and must be referenced to place the product within the Common Criteria evaluated configuration. The guidance documents are applicable for the version of SonicWall SMA claimed by this evaluation.

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

7 IT Product Testing

This section describes the testing efforts of the Evaluation Team. The information is derived from the SonicWall SMA v12.4 *Test Report* document. The purpose of this activity was to confirm that the TOE behaves in accordance with security functional requirements specified in the ST.

7.1 Developer Testing

NDcPP v2.2e evaluations do not require developer testing evidence for assurance activities.

7.2 Evaluator Independent Testing

A test plan was developed in accordance with the Testing Assurance Activities specified in the NDcPP v2.2e.

The formal testing activity was conducted between Nov 16, 2023, to August 7, 2024, with TOE installed in the Dekra lab located at 405 Glenn Dr, Suite 12, Sterling, VA 20164.

The Evaluator successfully performed the following activities during independent testing:

- Placed TOE into evaluated configuration by following the preparative procedures.
- Successfully executed the NDcPP v2.2e Assurance-defined tests.
- Planned and executed a series of vulnerability/penetration tests.

It was determined after examining the Test Report and full set of test results provided by the evaluators the testing requirements for PP NDcPP v2.2e are fulfilled.

7.3 Testing Topology

The TOE at the physical layer uses standard TCP/IP connectivity over a packet-switched Ethernet network. During testing standard networking equipment was used.

Note: The diagram below shows the components involved in the testing.

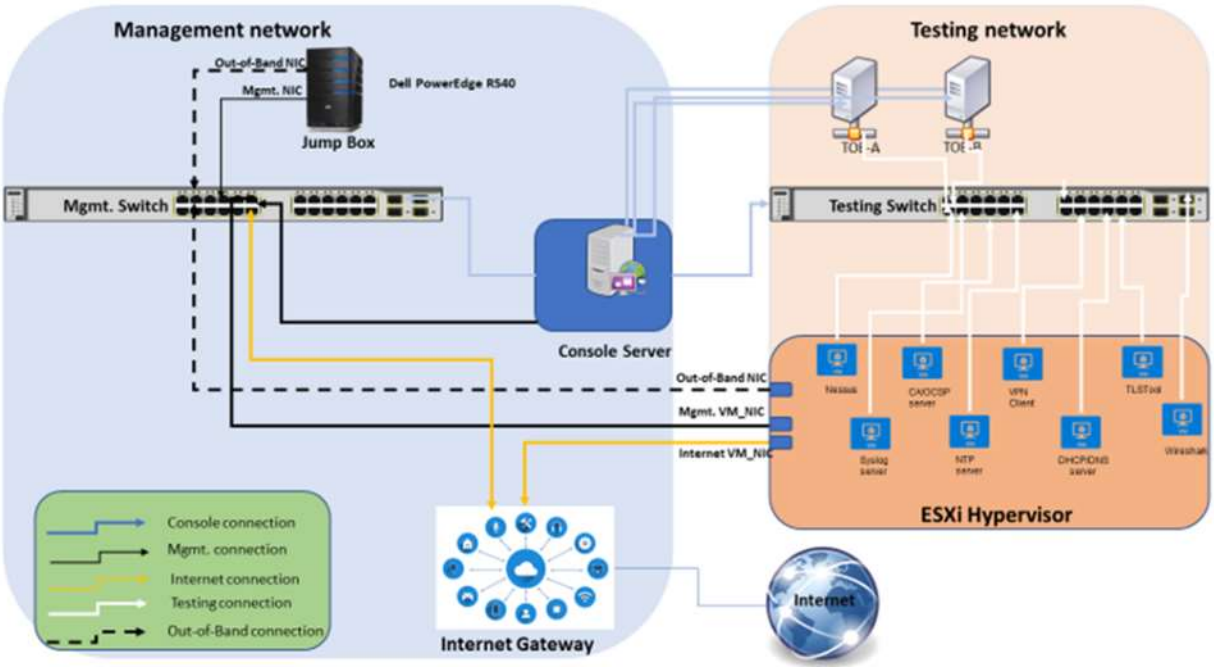


Figure 1: TOE Test Environment network diagram

Device	IP	Purpose
Tested platforms		
TOE-A	IPv4: 192.168.100.33 MAC: 2c:b8:ed:4a:39:b2	TOE is connected to the testing network
TOE-B	IPv4: 192.168.100.34 MAC:00:0c:29:a6:65:2f	Virtualized TOE that is connected to the testing network.
LAN switches		
S1	192.168.100.x/24	Port mirroring switch
Desktop servers (if not using virtualized environment)		
Audit Server and evaluator machine	IPv4: 192.168.100.61 MAC: 50:9a:4c:11:53:d6	OS: Kali GNU/Linux 2023.4 openssl 3.0.11 Function: audit server and evaluator machine
Rehtse	IPv4: 192.168.100.61 MAC: 50:9a:4c:11:53:d6	Rehtse Tool OS: Kali GNU/Linux 2023.4 Protocols: TLS 1.2 Function: TLS packets modification
CAs and OCSP Responders	IPv4: 192.168.100.61 MAC: 50:9a:4c:11:53:d6	OS: Kali GNU/Linux 2023.4 openssl 3.0.11 Function: Verify certificates status
Virtual servers (if using virtualized environment)		
Audit Server and evaluator machine	IPv4: 192.168.100.61 MAC: 00:0c:29:9f:a1:0a	OS: Kali GNU/Linux 2023.4 openssl 3.0.11 Function: audit server and evaluator machine

Device	IP	Purpose
Rehtse	IPv4: 192.168.100.61 MAC: 00:0c:29:9f:a1:0a	Rehtse Tool OS: Kali GNU/Linux 2023.4 Protocols: TLS 1.2 Function: TLS packets modification
CAs and OCSP Responders	IPv4: 192.168.100.61 MAC: 00:0c:29:9f:a1:0a	OS: Kali GNU/Linux 2023.4 openssl 3.0.11 Function: Verify certificates status
Network Traffic Capture		
Wireshark Laptop for physical TOE	IPv4: 192.168.100.61 MAC: 50:9a:4c:11:53:d6	OS: Kali GNU/Linux 2023.4 Wireshark 4.2.0 Function: Sniffing traffic
Wireshark Laptop for Virtual TOE	IPv4: 192.168.100.61 MAC: 00:0c:29:9f:a1:0a	OS: Kali GNU/Linux 2023.4 Wireshark 4.2.0 Function: Sniffing traffic
Remote Management		
Management Laptop for physical TOE	IPv4: 192.168.100.61 MAC: 50:9a:4c:11:53:d6	OS: Kali GNU/Linux 2023.4 nmap 7.94 Function: Management of the TOE
Management Laptop for Virtual TOE	IPv4: 192.168.100.61 MAC: 50:9a:4c:11:53:d6	OS: Kali GNU/Linux 2023.4 nmap 7.94 Function: Management of the TOE

Table 1: Testing Topology Identifiers

7.4 Test Hardware

The testing environment in the SEL has been implemented using the following hardware:

- Dell N3024 Switch with port-mirroring capabilities.
- Dell PowerEdge R350 used as Jump Box Server to access the local testing environment: running Windows 10 Professional
- Dell PowerEdge R550 server running VMWare ESXi 7.0 update 3.
- Personal computer:
    - Operative System: Kali Linux GNU/Linux Rolling 2023.4
    - RAM: 16GB
    - CPU: Intel® Core (TM) i7-7700 CPU @ 3.60GHz
    - Hard Disk: 2 TB
    - Ethernet Interface: Inter Corporation Ethernet Connection (5) I219-LM

7.5 Test Software

All testing was conducted using the following software:

- Burp Suite Pro 2023.12.1.3
- Nessus Vulnerability Scanner 10.6.4
- Nikto 2.5.0
- Nuclei v3.2.0
- Okteta
- Sqlmap 1.8.3#pip
- Wireshark v4.2.0 (64-bit)
- Rehtse tool v1.0
- OpenSSL 3.2.2-dev
- VPN Client Connected Tunnel

8 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all Evaluation Activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements.

The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluator determined the TOE to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Evaluation Activities specified in the [NDcPP].

The following evaluation results are extracted from the proprietary Evaluation Technical Report provided by the CCTL and are augmented with the validator's observations thereof.

8.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluator ensured the ST contained a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the TOE that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Evaluation Activities specified in the [NDcPP] in order to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit specified in the [NDCPP]. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

8.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit specified in the [NDCPP]. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

8.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit specified in the [NDCPP], as well as the Assurance Activities specified for ALC_CMC.1 and ALC_CMS.1. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit specified in the [NDCPP]. The evaluation team ran the set of tests specified by the Assurance Activities in the NDCPP and recorded the results in a Test Report, summarized in the Evaluation Technical Report and sanitized for non-proprietary consumption in the Assurance Activity Report.

The validator reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the [NDCPP], and that the conclusion reached by the evaluation team was justified.

8.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit specified in the [NDCPP]. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities was completed on August 5, 2024, and did not uncover any residual vulnerability.

The following search terms were utilized: Aopalliance Version 1.0 Repackaged As A Module, Apache Commons BeanUtils, Apache Commons Codec, Apache Commons Collections, Apache Commons Compress, Apache Commons Digester, Apache Commons FileUpload, Apache Commons IO, Apache Commons Lang, Apache Commons Logging, Apache Commons Text, Apache Log4J API, Apache Log4j, Apache Log4j SLF4J 2.0 Binding, Apache Struts, Apache Taglibs, Apache Velocity, Apache XML-RPC Client Library, Apache XML-RPC Common Library, Bean Validation API, Byte Buddy, ClassGraph, Eclipse Compiler for Java(TM), Expression Language 2.2 Implementation, Expression Language 3.0, Expression Language API, FreeMarker, HK2 API module, HK2 Implementation Utilities, Hibernate Commons Annotations, Hibernate ORM, Hibernate Validator, Hibernate Validator Annotation Processor, JAXB Runtime, JBoss Logging 3, JCommon, JFreeChart, Jackson-Datatype-JSR310, Jackson-JAXRS-base, Jakarta Activation, Jakarta Annotations API, Jakarta JSON Processing API, Jakarta Mail, Java API for Processing JSON (JSON-P), Java API for XML Web Services, Java Annotation Indexer, Java Native Access (JNA), JavaBeans Activation Framework API jar, JavaMail API (no providers), JavaMail API smtp provider, Javassist, Jersey, Jersey Inject HK2, Jetty :: ALPN :: JDK9 Server Implementation, Jetty :: ALPN Client, Jetty :: ALPN Server, Jetty :: Apache JSP, Jetty :: Servlet API and Schemas for JPMS and OSGi, Jetty Orbit :: JSP API, Jetty Orbit :: JSP Impl, Jetty: Java based HTTP/1.x, HTTP/2, Servlet, WebSocket Server, Log4J Commons Logging Bridge, MIME streaming extension, OSGi resource locator bundle, Quartz Enterprise Job Scheduler, SLF4J API Module, ServiceLocator Default Implementation, Spring Commons Logging Bridge, Spring Framework, acme4j Client, antlr, beanvalidation-api, c3p0DataSources/Resource Pools, dom4j: flexible XML framework for Java, image4j, io.swagger, istack common utility code runtime, jackson-annotations, jackson-core, jackson-databind, jackson-dataformat-yaml, jackson-jaxrs-json-provider, jackson-module-jaxb-annotations, jakarta.ws.rs-api, jakarta.xml.bind-api, java-classmate, javax.annotation API, javax.inject:1 as OSGi bundle, javax.json.bind-api, javax.persistence-api, javax.transaction API, jaxb-api, jboss-transaction-api_1.2_spec, jersey-container-servlet, jersey-container-servlet-core, jersey-core-server, jersey-declarative-linking, jersey-ext-entity-filtering, jersey-media-jaxb, jersey-media-json-jackson, jersey-media-multipart, jose4j, mariadb-java-client, mchange-commons-java, ognl, opencsv, swagger-core, swagger-integration, swagger-jaxrs2, swagger-models, ws-commons-util, acpid, libaudit1, libopts25, bind9-host, bash, libbz2-1.0, cabextract, libconfig-inifiles-perl, libxxhash0, libdbus-1-3, dash, isc-dhcp-client, libdebconfclient0, fonts-dejavu-extra, libfl2, libglib2.0-0, libgmp10, libc-bin, coreutils, diffutils, libmpfr6, cpio, grep, libsigsegv2, sed, tar, time, gawk, libgnutls30, libxtables12, nlohmann-json3-dev, less, libidn2-0, libtasn1-6, libattr1, libpam0g, locales, mariadb-client, netbase, ntpdate, libpcre3, libpcre2-8-0, libperl5.32, procps, qemu-guest-agent, readline-common, libsqlite3-0, libseccomp2, login, libfreetype6, pciutils, tzdata, vlan, xz-utils, libacl1, acpi-support-base, arping, at, base-files, bind9-dnsutils, bind9-libs, libbrotli1, bsdutils, libcjson1, ca-certificates, cron, daemontools, debianutils, runit-helper, dialog, dpkg, libext2fs2, libelf1, file, findutils, libfontconfig1, freecdb, gcc-10-base, ethtool, gzip, hostname, ifupdown, inetutils-ping, init-system-helpers, insserv, iproute2, ipset, libjansson4, libyaml-cpp0.6, libjq1, libjson-c5, kexec-tools, libkeyutils1, libkmod2, libaio1, libapt-pkg6.0, libarchive13, libboost-system1.74.0, libbpf0, libbsd0, libcap2-bin, libcap-ng0, libcrypt1, libdbi-perl, libdns-export1110, libdumbnet1, libedit2, libevent-2.1-7, libevent-core-2.1-7, libevent-extra-2.1-7, libevent-openssl-2.1-7, libevent-pthreads-2.1-7, libexpat1, libffi7, libfstrm0, libgcc-s1, libgdbm6, libhogweed6, libicu67, libipset13, libisc-export1105, libjpeg62-turbo, liblcms2-2, libmariadb3, libmaxminddb0, libmd0, libmnl0, libmspack0, libnet1, libnetfilter-conntrack3, libnettle8, libnfnetlink0, libnftnl11, libonig5, libp11-kit0, libpcap0.8, libpng16-16, libprocps8, libprotobuf23, libsemanage1, libsepol1, libss2, libstdc++6, libunistring2, liburing1, libuv1, libxml2, liblmdb0, logrotate,

logsave, lsb-base, lsof, liblz4-1, makedev, mawk, libmozjs-78-0, libncurses6, ncurses-bin, libdaxctl1, net-tools, libnftables1, libnghttp2-14, dmidecode, pci.ids, libpmem1, libpopt0, libprotobuf-c1, psmisc, rsync, libselinux1, sudo, libudev1, sysvinit-utils, libwrap0, tcpdump, thin-provisioning-tools, traceroute, ucf, ucspi-tcp, udev, util-linux, virtualbox-guest-additions-iso, libzstd1, Async, Chalk, Clone, D3.js, DataTables, Esprima, Gozala/querystring, JSHTTP's negotiator, Lightbox2, Node Cookie Parser, Qix-/color-convert, Raynos/for-each, Send for Node.js, Underscore.js, XPATH, ansi-styles, array-flatten, asn1.js, auth0, auth0-id-generator, available-typed-arrays, balanced-match, bn.js, body-parser, brace-expansion, bytes.js, call-bind, color-name, content-disposition, crypto-utils/random-bytes, datatables.net-dt, debug-js/debug, define-data-property, destroy, ee-first, encodeurl, es-define-property, es-errors, escape-html, etag, expressjs/accepts, expressjs/express, finalhandler, flowstate, forwarded, fs, function-bind, get-intrinsic, gopd, has-flag, has-property-descriptors, has-proto, has-symbols, has-tostringtag, hasown, http-errors, iconv-lite, inherits, is-arguments, is-callable, is-generator-function, is-typed-array, jake, js-sha256, js-yaml, jshttp/content-type, jshttp/fresh, jshttp/mime-types, mde (ejs), mde/filelist, media-typer, merge-descriptors, methods, mime, mime-db, minimalistic-assert, minimatch, moment/moment, ms.js, node-concat-map, node-cookie-signature, nodeca-argparse, nodejs Deprecate, nodejs/undici, object-inspect, ocsp, on-finished, parseurl, path-to-regexp, possible-typed-array-names, proxy-addr, qs - QS Querystring, range-parser, raw-body, safe-buffer, safer-buffer, saml2-js, samlp, serve-static, set-function-length, setprototypeof, side-channel, simple-lru-cache, sprintf.js, statuses, supports-color, toidentifier, type.is, uid-safe, unpipe, util, utils-flatten, utils-merge, valid-url, vary, which-typed-array, whitequark/ipaddr.js, xml-crypto, xml-encryption, xml-name-validator, xmlbuilder2, xtend, Click - Python Command Line Utility, ConfigObj, Flask, Jinja, MarkupSafe, PyYAML, Python Dialog, Python six, Werkzeug, ansi2html, anyio, blinker-pypi, dnslib, docopt, FastAPI, h11, httpcore, httpx, idna, importlib-resources, ipaddress, itsdangerous, jproperties, multidict, netifaces, orjson, psf-requests, pyOpenSSL, pyca/cryptography, pycparser, pydantic, pylockfile, pymysql, pyrsistent, python cffi, python-attrs, python-certifi, python-daemon (pypi), python-dateutil, python-json-patch, python-json-pointer, python-jsonschema, python-magic, python-multipart, python-typing-extensions, python3-charset-normalizer, sniffio, urllib3, uvloop, Spin.js, Linux Kernel, OpenSSL, apr-util, busybox, disconnect-mod_websocket, grub2, jQuery Splitter Plugin, jsTimezoneDetect, jsunzip.js, kkliuxu/xtree, libapache2-mod-proxy-msrpc, libesmtp, libntlm, mozilla-base64.js, noVNC, node-forge, ohdave/jscrypto, parted, Apache Ant, Apache CouchDB, Apache HTTP Server, Apache Portable Runtime, Cyrus SASL, GD, Heimdal Kerberos, Linux kernel crash utility, Net-SNMP, Node.js, OpenJDK, OpenLDAP, OpenSSH, Python programming language, QR-Code-generator, Redocly/redoc, Samba, abh's djbdns, chromium/hterm, cloud-init, curl, jQuery, jQuery UI, jitterentropy-library, jquery-i18n-properties, jshash, json-c, lvmteam/lvm2, lz4, nginx, nginx - njs, nginx-unit, open-vm-tools, swagger-ui, syslog-ng, Intel Core i5-7500, Intel Xeon E3-1275 v6, Intel Xeon Gold 5315Y, SMA 6210 / SMA 6210 Firmware, SMA 7210 / SMA 7210 Firmware, SMA 8200v / SMA 8200v Firmware.

The evaluator searched the following public vulnerability repositories:

The National Vulnerability Database at https://nvd.nist.gov/vuln

The CVE Details website at https://www.cvedetails.com/vulnerability-search.php

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the [NDCPP], and that the conclusion reached by the evaluation team was justified.

8.7 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the [NDCPP], and correctly verified that the product meets the claims in the ST.

9 Validator Comments

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Administrator Guide document listed in Section 6. No versions of the TOE and software, either earlier or later were evaluated. Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

10 Security Target

The security target for this product's evaluation is SonicWall SMA v12.4 Security Target version 1.2, August 14, 2024.

11 Acronyms

Acronym	Definition
CC	Common Criteria
CM	Configuration Management
CSP	Critical Security Parameter
ND	Network Device
FIPS	Federal Information Processing Standard
IT	Information Technology
NIST	National Institute of Standards and Technology
OE	Operational Environment
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation

TSF	TOE Security Function

12 Terminology

Terminology	Definition
Common Criteria Testing Laboratory (CCTL)	An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
Conformance	The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
Evaluation	The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
Evaluation Evidence	Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
Feature	Part of a product that is either included with the product or can be ordered separately.
Target of Evaluation (TOE)	A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
Validation	The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
Validation Body	A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

13 Bibliography

URLs

[1] Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap-ccevs.org/cc-scheme).

[2] Dekra Cybersecurity Certification CCTL (https://www.dekra.us/).

CCEVS Documents

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.

Other evaluation documents

1. SonicWall SMA 12.4 Security Target v1.2 August 14, 2024
2. SMA 12.4 Administration Guide
3. SonicWall Secure Mobile Access 12.4 Common Criteria Document version 6.0
4. SonicWall SMA v12.4.3 Third-Party Libraries Vulnerability Analysis Report v1.1, August 2024
5. SonicWall SMA v12.4.3 Test Report version 0.5 August 2024
6. Assurance Activity Report for SonicWall Secure Mobile Access v12.4 Version 0.5 August 2024